UNCLAS SECTION 01 OF 03 NEW DELHI 001520

SIPDIS

SENSITIVE

STATE/PM FOR MICHELE MARKOFF
DOD FOR OASD/NII TIM BLOECHL

E.O. 12958: N/A
TAGS: KCIP TINT KCRM PREL PGOV IN GOI
SUBJECT: GOI UPBEAT ON CYBER-COOPERATION, SERIOUS ABOUT CYBER-TRAINING

REF: A. NEW DELHI 709
¶B. NEW DELHI 550
¶C. 04 NEW DELHI 8060
¶D. 04 NEW DELHI 7026

¶1. (SBU) Summary: In a brief February 22 meeting, National Security Council Secretariat Joint Secretary Arvind Gupta and Deputy Director (Information Security) Commander Mukesh Saini were upbeat on US-India cybersecurity cooperation, clarified the objective of the upcoming April 18-19 Cybersecurity Seminar in New Delhi, and demonstrated that the GOI is educating the Indian legal system on cybersecurity and related issues. They also outlined some of the strengths and weaknesses of the Indian IT Act (2000) and described the December 17 arrest of Baazee.com CEO Avnish Bajaj as a case of inadequate police training on IT issues -- an area they say they are trying to improve. Gupta also outlined how the NSCS became the GOI's cybersecurity nodal agency. Separately, President Kalam in a recent address at the National Judicial Academy underlined the importance of India having a robust cybersecurity regime. End Summary.

GOI Very Upbeat on Cyber-Cooperation

¶2. (SBU) J/S Gupta opened February 22 discussion by with Poloff comparing the upcoming April 18-19 Cybersecurity Seminar (Ref B) in New Delhi to last November's Cybersecurity Forum: "We shared our concerns then, now we will share information and cooperation." He also welcomed what he termed "growing IT interdependence" as part of expanding the overall US-India relationship, adding that, "The logic of markets and the logic of globalization make cybersecurity cooperation a necessary win-win situation."

Goal of April Seminar

¶3. (SBU) Gupta then explained that the goal of the April seminar is to address US concerns regarding Indian legal issues in the cybersecurity arena, including for example the IT Act (2000), the Evidence Act, the Criminal and Civil Penal Codes, digital evidence, data privacy, and confidentiality. "I was surprised, for example, on how far Indian industry was ahead of law enforcement regarding due diligence," he expanded, noting that firms need to be very sensitive due to their high level of accountability.

Serious about Cybersecurity Legal Training

¶4. (SBU) Although Gupta had no data on how much is budgeted nationally for cybersecurity, he pointed out that related classes are taught at the Indian Institutes of Science and that the Indian Institutes of Technology offer both courses and research opportunities. The Department of Information Technology also funds cybersecurity research projects, as does the Banking Research Institute, he added. Cdr. Saini reiterated GOI interest in on-site co-training in both India and the US (Ref D), and on cooperation in tackling the "hard problems" list.

¶5. (SBU) Gupta told Poloff that the National Judicial Academy in Bhopal is training new and current judges in cyberlaw. The training includes a layperson's overview of the technological possibilities and limits of IT, as well as training on India's IT laws. Separately, the "Hindustan Times" on February 25 reported that the first class of a dozen lower court judges in New Delhi had just completed a three-day seminar on IT and law as part of its obligations as a signatory to the UN Commission on International Trade Law. Their program included overviews of steganography, encryption, digital signatures, website defacing, and recovery of digital data as evidence. Gupta hopes to have some recently-cybertrained judges attend the April Seminar.

¶6. (U) Separately, in a February 19 address to the Judicial Colloquium on Science, Laws, and Ethics at the National Judiciary Academy, President AJP Abdul Kalam offered the following remarks on modernizing India's cyber laws and cyber

capabilities: "India's cyber laws need to look at the fact that nowadays nations are electronically connected, with all their electronic assets. Defense and national security establishments will be targets for cyber attacks during a conflict. In such a situation, a country can be defeated without a missile or aircraft attack, just through intelligent cyber war. Hence it is essential to generate a model of the connected economic and defense security system as a cyber/electronic network. This will reveal the need for a new policy with redundancy and restriction of external connectivity and external partnership of certain vital establishments."

IT Act "India's Most Comprehensive Cybersecurity Tool"

¶7. (SBU) The most comprehensive legal tool New Delhi has for cybersecurity is the IT Act (2000), Gupta told Poloff. This statute being revisited, he said, and may be amended to account for changes in technology and to incorporate lessons learned, but it is "robust enough and impartial enough to address the situation" and it "rests on a solid foundation of Indian civil and criminal law traditions." Gupta underlined that the problems with the IT Act were that law always lags behind technology, and that law is bound by borders while IT is not. "In the UK, Australia, the US, the problems are the same but the laws are different," he added. Gupta expected that the US delegation to the April seminar would have many questions regarding the IT Act.

Baazee.com Arrest Blamed on Inadequate Training

¶8. (SBU) When asked if the IT Act would be amended in light of the December 17 arrest of Baazee.com CEO Avnish Bajaj (Ref C), Gupta answered that his office was surprised when the arrest happened, and he noted that it drew extensive criticism from the Indian IT sector as well as from foreign IT firms. Saini commented that the issue was not the IT Law itself but the poor police training that led to, as he viewed it, "improper implementation of the law." Gupta continued that a major drawback with the IT Law is that even after almost five years it lacks a substantial body of case law to guide the police and the courts. Observing that "Personally, I think the arrest was a mistake," Gupta reiterated the importance of training judges, police, investigators, and attorneys on the law, and asked if we could provide US cybercrime cases that could be used as references as India develops its own case law. (Note: Mission is following up on this. End note.) He reiterated that the law is being revisited and the case is currently in the courts where it will continue to unfold. He expected the US delegation in April to discuss this case as well.

Where the NSCS Fits in the GOI

¶9. (SBU) Gupta concluded by outlining NSCS's overarching function as supporting the NSC and NSA MK Narayanan (Ref A), and providing independent inputs on both traditional and non-traditional security issues, including cybersecurity. As such, the NSCS takes the lead in coordinating with agencies throughout the GOI on national information security policy, including the Department of Telecommunications, the Department of Information Technology, and the Ministries of Law and Home Affairs, as well as academia and private industry. In the area of international cybersecurity cooperation, he said that New Delhi's relations with Washington are "the strongest we have;" although in this meeting he only specified cybersecurity cooperation with China, in the past our GOI cybersecurity interlocutors have referenced relationships with Canada, Russia and Israel (Ref D).

Comment

¶10. (SBU) The brief NSCS conversation and President Kalam's remarks demonstrate that the GOI understands that the US-India Cybersecurity Forum can provide New Delhi with the training and contacts to help it nourish India's growing information economy and make its governmental organization and policies regarding cybersecurity more sophisticated. It provides another strand in the web of functional relations that strengthens the US-India government-to-government dynamic. The US-India cybersecurity relationship will require careful nurturing from both sides to ensure the working groups fulfill their potential, as well as complete their stated goals and objectives. However, the groundwork has been laid for a long-standing and robust cyber exchange with important political and commercial benefits.
MULFORD